Data Breach Incident Procedures

Introduction

The purpose of these procedures are to provide the basis of appropriate response to a Data Breach. A Data Breach is defined as an attempt to access data that threatens the confidentiality, integrity, and availability of the district's information systems and the networks that deliver the information. The Data Breach Incident Procedures provides a process for documentation, and appropriate reporting to internal and external resources. Finally, the procedures establishes responsibility and accountability for all steps in the process of addressing computer security incidents. Ware Shoals School District 51/Greenwood 51 is responsible for Personal Data about our users, employees, clients, suppliers and other individuals for a variety of business and educational purposes. Ware Shoals School District 51/Greenwood 51 is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

Scope

The Data Breach Incident Procedure applies to all resources that have or gain access to Ware Shoals School District 5/Greenwood 51 information systems and network. District resources include faculty and staff members, students, guests, and other members. This procedure also includes computing or network devices owned, leased, or otherwise controlled by the district. Additionally, incidents involving confidential information apply to any computing or network device, regardless of ownership, on which confidential or restricted information is stored or by which access to confidential or restricted information might be gained. (Examples include but are not limited to: a home computer containing confidential data, a mobile device on which credentials are stored which could be used to access confidential data, any other technology housed in an off-site facility.)

Data Breach Incident Action Statement

The Incident Response Procedure is as follows:

- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to an incident.
- The objectives for management should be agreed upon, and it should be ensured that those responsible for an incident understand the district's priorities for handling such incidents.
- Security incidents should be reported through appropriate management channels as quickly as possible.
- Employees, students, guest and others using the district's information systems and services are required to note and report any suspected security weakness in systems or services.
- Security incidents should be assessed, and it should be decided if they are to be classified as security incidents.
- Knowledge gained from analyzing and resolving security incidents should be used to reduce the likelihood or impact of future incidents.
- Procedures should be defined and applied for the identification, collection, acquisition, and preservation of information, which can serve as evidence.
- Constraints may be imposed by non-disclosure agreements depending on the nature of the security incident.
- Communication channels should be established well in advance of any security incident.

Data Breach Incident Training

All staff receive training on this procedure annually. New staff will receive training as part of the induction process. Further training will be provided at least e*very y*ear or whenever there is a substantial change in the law or our procedure. Training is provided through Safe Schools training and on-site instruction. These trainings cover the applicable laws relating to data protection, and any district related policies and procedures. Completion of training is compulsory.

Data Breach Incident Causes:

Human Error

- Loss of computing devices (portable or otherwise)
- Handling data in an unauthorized way (downloading a local copy of personal data)
- Unauthorized access or disclosure of personal data by employees
- Improper disposal of personal data
    - (hard disk, storage media, or paper documents containing personal data sold or discarded before data is properly deleted)

Malicious Activities

• Hacking incidents / Illegal access to databases containing personal data

• Hacking to access unauthorized data via the Coaching App or API

• Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal data Scams that trick staff into releasing personal data of individuals

Computer System Error

• Errors or bugs in Ware Shoals School District 51/Greenwood 51 software applications

• Failure of cloud services, cloud computing or cloud storage security

Reporting a Data Breach Incidence

All district employees have an obligation to report actual or potential data protection compliance failures. Ware Shoals School District 51/Greenwood 51 requires:

- District employees to report suspected security incidents to the district's incident response capability within 24 hours
- Reporting to immediate supervisor and to the district Safety Coordinator
- Reporting of security incident information to the district's information technology helpdesk.

The intent of this control is to address both specific incident reporting requirements within the district and the formal incident reporting requirements for the district. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain security concerns.

Handling of Data Breach Incident

All incident response personnel for Ware Shoals School District 51/Greenwood 51 will:

- Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Ware Shoals School District 51/Greenwood 51 recognizes that incident response capability is dependent on the capabilities of district information systems and the mission/business processes being supported by those systems. Therefore, the district considers incident response as part of the definition, design, and development of mission/business processes and information systems.

Data Breach Incident Monitoring

Ware Shoals School District 51/Greenwood 51 response personnel continue monitor and focus on security and unusual network activity that could indicate a data breach incident.

Documenting information system security incidents is critical to improving future incident response procedures and policies. Examples of details about incidents are, but not limited to, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling incident information obtained from a variety of sources. Examples of those sources are incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Data Breach Incident Response Personnel

Under the supervision of the Superintendent, the Ware Shoals School District 51/Greenwood 51 Data Breach Response Personnel consists of the Director of Technology, the District Safety Coordinator and the Chief Academic Officer. The Data Breach Incident Response Personnel maintain the responsibility to make all time-critical decisions on steps taken to contain and manage the data breach incident.

The Data Breach Incident Personnel should immediately be alerted of any confirmed or suspected data breach via email,

The notification should include the following information, where available:

- Extent of the data breach
- Type and volume of personal data involved
- Cause or suspected cause of the breach
- Whether the breach has been rectified
- Measures and processes that the organization had put in place at the time of the breach
- Information on whether affected individuals of the data breach were notified and if not, when the organization intends to do so

Where specific information of the data breach is not yet available, Ware Shoals School District 51/Greenwood 51 should send an interim notification comprising a brief description of the incident.

Notifications made by organizations or the lack of notification, as well as whether organizations have adequate recovery procedures in place, will affect supervising authorities' decision(s) on whether an organization has reasonably protected the personal data under its control or possession.

Data Breach Incident Procedure Plan

Notification of a (suspected or confirmed) data breach to the Data Breach Incident Personnel should immediately activate the Data Breach Incidence Response plan.

Ware Shoals School District 51/Greenwood 51 Data Breach Incident Response Personnel and response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

Data Breach Incident Confirmation

The Data Breach Incident Response Personnel should act as soon as it is aware of an incident. Where possible, it should first confirm that the data breach incident has occurred. It may make sense for the Data Breach Incident Response Personnel to proceed contain the incident on the basis of an unconfirmed reported data breach, depending on the likelihood of the severity of risk.

Data Breach Incident Containment

The Data Breach Incident Response Personnel should consider the following measures to contain the incident, where applicable:

- Shut down the compromised system that led to the data breach.
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (Remotely disabling / wiping a lost notebook containing personal data of individuals.)
- Prevent further unauthorized access to the system,
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

Data Breach Incident Reporting

Ware Shoals School District 51/Greenwood 51 is legally required to notify affected individuals if their personal data has been compromised. This will encourage individuals to take preventive measures to reduce the impact of the data breach, and also help our district to rebuild consumer/community trust.

Who to Notify:

- Notify individuals whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify relevant authorities (police) should criminal activity be suspected and evidence for investigation should be preserved (hacking, theft or unauthorized system access by an employee.)

When to Notify:

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved

How to Notify:

- Use the most effective *w*ays to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:

- How and when the data breach occurred, and the types of personal data involved in the data breach.
- What actions accomplished in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
- Contact details and how affected individuals can reach the organization for further information or assistance (helpline numbers, email addresses or website).

Data Breach Incident Response Compliance

All employees of Ware Shoals School District 51/Greenwood 51 are required to comply with the above mentioned procedures. Violations of these procedures are treated like other allegations of wrongdoing with Ware Shoals School District 51/Greenwood 51. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action per applicable Ware Shoals School District 51/Greenwood 51 policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.